5/206.19 FACIAL RECOGNITION TECHNOLOGY

Facial recognition technology involves the ability to examine and compare distinguishing characteristics of a human face through the use of biometric algorithms contained within a software application. This technology can be a valuable investigative tool to detect and prevent criminal activity, reduce an imminent threat to health or safety, and help in the identification of persons unable to identify themselves or deceased persons.

The LVMPD has established the capability to conduct facial recognition searches in support of law enforcement activities. This capability is primarily available through the facial recognition program, which is managed by the Technical Operations Section (Tech Ops).

PURPOSE

This policy provides LVMPD personnel with guidance and principles for the collection, access, use, dissemination, retention, and purging of images and related information applicable to the implementation of a facial recognition program. This policy will ensure that all facial recognition searches are consistent with authorized purposes while not violating the privacy, civil rights, and civil liberties of individuals. Further, this policy will delineate the manner in which requests for facial recognition information is received, processed, catalogued, and responded to.

This policy assists LVMPD personnel in:

1. Increasing public safety and improving state, local, tribal, territorial, and national security.
2. Minimizing the threat and risk of injury to specific individuals.
3. Minimizing the threat and risk of physical injury or financial liability to law enforcement and others responsible for public protection, safety, or health.
4. Minimizing the potential risks to individual privacy, civil rights, civil liberties, and other legally protected interests.
5. Protecting the integrity of criminal investigatory, criminal intelligence, and justice system processes and information.
6. Making the most effective use of public resources allocated to public safety entities.

GENERAL USE

All deployments of facial recognition must be for official use for a law enforcement purpose only. A request for facial recognition analysis to Tech Ops will only be for official investigations that have a criminal predicate or an articulated public safety concern. The following are the authorized uses of facial recognition applications:

1. A reasonable suspicion that an identifiable individual has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal conduct or activity.
2. An active or ongoing criminal or homeland security investigation.
3. To mitigate an imminent threat to health or safety through short-term situational awareness surveillance or other means.
4. To assist in the identification of a person who lacks capacity or is otherwise unable to identify himself (such as an incapacitated, deceased, or otherwise at-risk person).
5. To investigate or corroborate tips and leads.
6. For comparison to determine whether an individual may have obtained one or more official state driver's licenses or identification cards that contain inaccurate, conflicting, or false information.
7. To assist in the identification of potential witnesses or victims of violent crime.
8. To support law enforcement in critical incident responses.

This policy was also established to ensure that all images are lawfully obtained, including facial recognition probe images obtained or received, accessed, used, disseminated, retained, and purged according to LVMPD record retention policies. This policy applies to:

1. Images contained in a known identity face image repository and its related identifying information.
2. The facial recognition search process.

3. Any results from facial recognition searches that may be accessed, searched, used, evaluated, retained, disseminated, and purged by the LVMPD.
4. Lawfully obtained probe images of unknown suspects that have been added to unsolved image files pursuant to authorized criminal investigations.

FACIAL RECOGNITION SEARCHES

Facial recognition searches may only be performed by persons who have completed training and only during the course of lawful duties, in furtherance of a valid law enforcement purpose and in accordance with this policy. Valid law enforcement purposes include but are not limited to the following activities:

1. For persons who are detained for offenses that warrant arrest or citation.
2. For persons who are subject to lawful identification requirements and are lacking positive identification in the field.
3. For a person who an officer reasonably believes is concealing his true identity and has a reasonable suspicion the individual has committed a crime other than concealing his identity.
4. For persons who lack capacity or are otherwise unable to identify themselves and who are a danger to themselves or others.
5. For those who are deceased and not otherwise identified.

Authorized and trained LVMPD personnel may only perform a facial recognition search during the course of lawful duties, in accordance with LVMPD established authorized uses and when one of the following conditions exist:

1. Public Place: In accordance with applicable law, the individual's image is captured in a public place for the purpose of identification and the individual has no reasonable expectation of privacy. The LVMPD will not authorize the collection of the individual's face image when the individual raises an objection that is recognized by law (e.g., religious objection).
2. Consent: The individual consents to have his image captured for the purpose of identification. The individual may withdraw consent at any time. If consent is withdrawn and neither of the other conditions applies, then use of a facial recognition search is not authorized and the search must stop immediately.
3. Incapacitation, Defect, or Death: When an individual is unable to provide reliable identification because of physical incapacitation or defect, mental incapacitation or defect, or death, and an immediate identification is needed to assist the officer in the performance of his lawful duties.

PROGRAM MANAGEMENT

Tech Ops will be responsible for deploying, managing, and controlling access to the facial recognition program. Tech Ops Lieutenant, or designee, will ensure that access to facial recognition software is restricted to LVMPD personnel in assignments that require access to the facial recognition system or searches. Facial recognition will only be used for official and legitimate law enforcement purposes. Any misuse of facial recognition data may result in disciplinary action, up to termination.

The LVMPD is authorized to access and perform facial recognition searches utilizing the following external repositories:

1. Mugshots database.
2. Vigilant Solutions FaceSearch database.

Before access to the LVMPD facial recognition system is authorized, the LVMPD will require individuals to participate in training on the implementation of and adherence to this facial recognition policy.

PROCEDURE

All requests for facial recognition analysis will require a "probe photo." A probe photo is a still photograph depicting the face of the subject whose identity is unknown. For the most accurate results, this photo needs to be of the best quality possible and ideally an original, not a copy of a copy.

Requesting investigator will:

1. Submit a formal request via email to Tech Ops, which will include the following:
   a. Probe photograph of an unknown subject and descriptors provided by victim/witnesses (estimated age, height, weight, race, tattoos or other unique identifiers).
   b. Event number.
   c. Nature of the crime.
   d. Investigator's assignment.

Tech Ops FaceSearch Examiner will:

2. Analyze, review, and evaluate the quality and suitability of probe images, to include factors such as the angle of the face image, level of detail, illumination, size of the face image, and other factors affecting a probe image prior to performing a facial recognition search.
3. Initially run probe images without filters, using a filtered search as a secondary search, if needed. In some cases, enhancements may be considered after running an image as is against the image repository.
4. In the automated search, most likely candidates are returned to the requestor ranked in order based on the similarity or confidence level.
5. The resulting candidates, if any, are then manually compared with the probe images and examined by an authorized, trained examiner from Tech Ops. Examiners shall conduct the comparison of images, biometric identifiers, and biometric information in accordance with their training.
   a. If no likely candidates are found, the requesting entity will be informed of the negative results. In the case of a negative result, the images examined by the examiner will not be provided to the requesting entity.
   b. If candidates are found, examiners will submit the search and subsequent examination results for a peer review of the probe and candidate images for verification by another authorized, trained examiner.

FACIAL RECOGNITION RESULTS

All entities receiving the results of a facial recognition investigation must be cautioned that the resulting candidate images do not provide positive identification of any subject and are considered advisory in nature as an investigative lead only. Resulting candidate images do not establish probable cause to obtain an arrest warrant without further investigation and other facts or evidence. Any possible connection or involvement of the subject to the investigation must be determined through additional investigative methods. (8/18)■